

S/N 09/304,444

Response to Office Action Dated 12/02/2004

REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application. This amendment is believed to be fully responsive to all issues raised in the 12/02/2004 Office Action.

In the Claims:

Previously, claims 1 and 3—19 were pending.

Claims 1, 4, 5, 7, 11 and 15 are currently amended.

Claim 9, 10, 13 and 14 are canceled.

No claims are added.

Claims 3, 6, 8, 12, 16, 18 and 19 are original.

Accordingly, claims 1 and 3—8, 11—12, 15—19 are pending.

Section 103 Rejection of the Claims

Claims 1, 3—16 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,623,637, hereinafter "Jones" in view of U.S. Patent No. 6,353,885, hereinafter "Herzi." The Applicants respectfully traverse the rejection and request that the rejection be reconsidered and withdrawn.

Claims 1, 7 and 11 were amended to include material previously recited in claims 4, 9 and 10, respectively. Accordingly, the rejection of claims 1, 7 and 11 will address the rejections of claims 4, 9 and 10, respectively.

Claim 1 recites in a paragraph moved from claim 4, "wherein the memory device stores a public key and the smart card stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated."

Claims 7 and 11 were similarly amended to recite elements formerly found in claims 9 and 10.

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 The rejection of claims 4, 9 and 10 (and therefore current claims 1, 7 and
2 11) was based on two passages in the Jones reference, i.e. column 9 lines 22—37
3 and column 9 lines 5—15. The cited passages in column 9 of Jones involves two
4 paragraphs, lines 1—21 and 22—37. In the first paragraph, at column 9 lines 1—
5 21, Jones does not disclose public and/or private keys. Instead, Jones discloses a
6 challenge-and-response system by which a user of a local computer having the
7 PCMCIA card can gain access to capabilities of a remote computer. In particular,
8 the access code (password) required to access the remote computer is stored in a
9 password-protected PCMCIA card (col. 9, lines 6—10). Random numbers are
10 used within the challenge-and-response exchange to protect the access code from
11 interception by those monitoring the local and remote computers (col. 9, lines
12 11—21).

13 In the second paragraph, column 9 lines 22—37, Jones discloses how the
14 local computer may request transmission of encrypted data, after the challenge-
15 and-response sequence have proven the identity of the local / host (i.e. host of the
16 PCMCIA card) computer to satisfaction of the remote computer. The data is
17 encrypted according to a public key by the remote computer, and a private key is
18 used by the host (of the PCMCIA card) to decrypt the data. Jones notes that more
19 than one computer may send data using the public key to encrypt that data to be
20 sent.

21 The Patent Office takes the position that access to the remote computer by
22 the host computer is provided after the public and private keys have been shown to
23 be associated. (See rejection of claims 4, 9 and 10, middle of page 4 of document
24 mailed 12/02/2004. Note however, that *the Patent Office takes a conflicting*
25 *position on page 8, line 7—9 of the document mailed 12/02/2004, when the Patent*

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 *Office indicated that Jones "does not disclose ... verifying compatibility of the*
2 *public key and the private key."*)

3 However, what Jones really disclosed was that successful completion of a
4 challenge-and-response exchange between the remote and host computers, and
5 transmission of data from the remote computer (wherein the data was encoded by
6 the public key) to the host computer (wherein the data was decoded by the private
7 key). Accordingly, Jones discloses only conventional use of passwords (the
8 challenge and response) along with conventional use of a public key to encrypt
9 data and of a private key to decrypt the data.

10 Therefore, Jones discloses the typical use of public/private key
11 cryptography, wherein the public and private keys are used to encrypt and decrypt
12 data, respectively. Jones fails to disclose a process wherein verification of the
13 association between a public key and a private key is used to provide access to
14 data.

15 Accordingly, Jones does not disclose the recited elements of the claim, and
16 therefore the Applicant respectfully requests that the rejection be removed from
17 claims 1, 7 and 11.

18 Claims 3, 4 and 8 depend from claims 1 and 7, and are allowable by virtue
19 of this dependence, as well as for reasons associated with the elements recited by
20 each claim. Accordingly, the Applicant respectfully requests that these claims be
21 allowed to issue.

22 Claim 5 recites in part "authenticate the public key stored on the memory
23 device using the private key." The argument with respect to claims 1, 7 and 11,
24 above, is incorporated herein by reference. The Patent Office argues that Jones
25 discloses the above-recited passage, and points to Jones' column 9, lines 24 -42.

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 As discussed with respect to claims 1, 7 and 11, Jones discloses use of a public
2 key to encrypt (Jones, column 9, lines 28—29) and uses the private key to decrypt
3 (column 9, lines 29—31). This is the conventional use of public/private key
4 inscription.

5 In contrast, claim 5 recites the use of public and private keys in an
6 authentication roll, as opposed to the conventional use of such keys disclosed by
7 Jones, i.e. data encryption. Accordingly, elements recited by claim 5 are not shown
8 by Jones, and the Applicant respectfully requests that the rejection of claim 5 be
9 removed.

10 Claim 6 depends from claim 5, and is allowable by virtue of this
11 dependence, as well as for reasons associated with the elements recited in claim 6.
12 Accordingly, the Applicant respectfully requests that claim 6 be allowed to issue.

13 Claim 12 depends from claim 11, and is allowable by virtue of this
14 dependence, as well as for reasons associated with the elements recited by each
15 claim. Accordingly, the Applicant respectfully requests that claim 12 be allowed
16 to issue.

17 Claim 15 was amended, as was claim 1, to include elements from claim 4.
18 Accordingly, claim 15 is allowable for substantially the same reasons as claim 1,
19 and the arguments presented above are incorporated herein by reference.

20 Claim 16 depends from claim 15, and is allowable by virtue of this
21 dependence, as well as for reasons associated with the elements recited by claim
22 16. Accordingly, the Applicant respectfully requests that claim 16 be allowed to
23 issue.

24 Claim 17 is rejected under 35 U.S.C. §103(a) as being unpatentable over
25 Jones in view of U.S. Patent No. 5,987,138, hereinafter “Gilbert.” The Applicants

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 respectfully traverse the rejection and request that the rejection be reconsidered
2 and withdrawn.

3 Claim 17 recites, in part,
4 “verifying compatibility of the public key and the private key; and
5 “allowing, in response to the verified compatibility, access to the user data
6 on the portable memory device.”

7 The Gilbert reference discloses an identification and/or signature process
8 whereby a claimant is able to convince a verifier that the claimant is who the
9 claimant represents to be. This is a one-way process, in that the claimant does not
10 verify who the verifier is, but wherein the verifier does verify who the claimant is.
11 *Accordingly, the issue addressed by Gilbert is not the compatibility of the public
12 and private key; instead, Gilbert addresses validity of the identity of the claimant.*

13 Gilbert discloses a series of steps wherein questions and answers are passed
14 between the claimant and the verifier, ultimately providing a level of assurance to
15 the verifier of the claimant’s identity. *However, in none of the questions does
16 Gilbert verify the compatibility of the public key and the private key; instead,
17 Gilbert verifies the identity of one party to the satisfaction of the other party.*

18 The Patent Office suggests that the verifier sends random numbers, and that
19 these numbers are used in the process that verifies the claimant’s identity.
20 However, the Applicant’s claim does not recite random numbers or verifying an
21 identity of one party, but instead recites the compatibility of two keys.

22 Accordingly, Gilbert discloses a method by which one party (the claimant)
23 can verify its identity to the satisfaction of the other party (the verifier). This is
24 not the same as “verifying compatibility of the public key and the private key,”
25 which involves verification that each key is compatible with (as opposed to known

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 to) the other. Accordingly, the Applicant respectfully requests that the rejection to
2 claim 17 be removed, and that claim 17 be allowed to issue.

3 **Claims 18 and 19** are rejected under 35 U.S.C. §103(a) as being
4 unpatentable over Jones and Herzi, in view of U.S. 6,266,416, hereinafter
5 "Sigbjornsen." The Applicants respectfully traverse the rejection and request that
6 the rejection be reconsidered and withdrawn.

7 Claims 18 and 19 recite "authenticating the public key using the private
8 key," and "authenticating, at the smart card, the device-resident key using the
9 card-resident key," respectively.

10 Column 9, lines 1—21 of Jones discloses a challenge-and-response
11 exchange wherein a password on the PCMCIA card is used to access designated
12 functions on the remote computer. Thus, a conventional use of passwords is
13 disclosed.

14 Column 9, lines 22—37 of Jones discloses encrypted data from the remote
15 computer using the public key on the host computer and the private key on the
16 smartcard. Thus, conventional use of public and private key cryptography is
17 disclosed for encoding data for secure transmission.

18 The Patent Office cited column 9 of Jones for allegedly disclosing card key
19 and device key authentication, as well as public key and private key association.
20 Since this rejection is similar to that of claim 1, that response is incorporated
21 herein, and the below comments are also to be added to that response.

22 In particular, the Patent Office suggests that lines 5—37 disclose
23 verification of the association of the keys. However, the first paragraph of column
24 9 actually discloses a challenge-and-response password procedure wherein the
25 host of the PCMCIA card gains access to functionality on the remote computer,

S/N 09/304,444

Response to Office Action Dated 12/02/2004

1 and the second paragraph of column 9 discloses use of public and private key
2 cryptography to transfer data from the remote computer to the host computer.

3 Sigbjornsen, column 9 lines 44—49, discloses the use of public and private
4 key cryptography to decrypt sections of code that have been encrypted to thwart
5 use without permission. Thus (as seen in Fig. 2 of Sigbjornsen) a segment of the
6 software is encrypted. (By encrypting only part of the software, decryption
7 overhead is reduced.) Lines 44—49 describe how 44—57 describe how the
8 decryption is performed.

9 Thus, neither reference discloses, “authenticating the public key using the
10 private key.” Accordingly, the Applicant respectfully requests that the rejection to
11 claims 18 and 19 be removed.

12
13
14
15
16
17
18
19
20
21
22
23
24
25

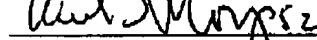
S/N 09/304,444

Response to Office Action Dated 12/02/2004

Conclusion

Claims 1 and 3—8, 11—12, 15—19 are in believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is encouraged to contact the undersigned attorney to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

By: 
David S. Thompson
Reg. No. 37,954
Attorney for Applicant

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201
Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979